

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-117173

(43)公開日 平成10年(1998) 5月6日

(51)Int.Cl.<sup>9</sup>

識別記号

F I

H 0 4 H 1/00

H 0 4 H 1/00

F

H 0 4 K 1/00

H 0 4 K 1/00

Z

H 0 4 N 7/16

H 0 4 N 7/16

C

7/167

7/167

Z

審査請求 未請求 請求項の数11 O L (全 10 頁)

(21)出願番号

特願平8-269938

(22)出願日

平成8年(1996)10月11日

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72)発明者 早川 和宏

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 福永 博信

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 渡部 智樹

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74)代理人 弁理士 若林 忠

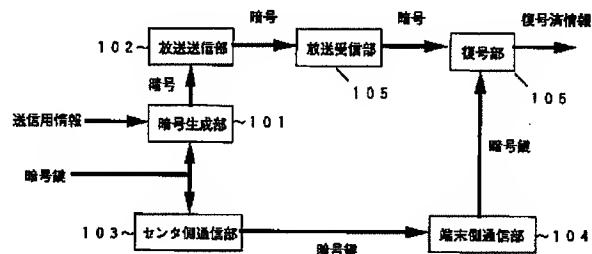
最終頁に続く

(54)【発明の名称】 情報配信装置および情報受信装置

(57)【要約】

【課題】 暗号化された情報を多数の利用者に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険を小さくする。

【解決手段】 暗号生成部101は送信用情報と暗号鍵を受け取り、送信用情報を暗号化して出力する。放送送信部102は暗号を受け取り不特定多数に対して放送する。センタ側通信部103は暗号鍵を受け取り、通信路を通じて送信する。端末側通信部104は通信路を通じて暗号鍵を受け取り、出力する。放送受信部105は放送された暗号を受信し出力する。復号部106は暗号と暗号鍵を受け取り、復号済み情報を出力するが、暗号鍵が入力されない場合は動作を行わない。



**【特許請求の範囲】**

【請求項 1】 情報を暗号化して配信する情報配信装置であって、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された前記情報を含む情報を放送する放送送信手段と、前記暗号鍵を通信路を通じて送信する暗号鍵送信手段とを有する情報配信装置。

【請求項 2】 情報を暗号化して配信する情報配信装置であって、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された前記情報を含む情報を放送する放送送信手段と、前記暗号鍵を含む照合情報を通信路を通じて送信する照合情報送信手段とを有する情報配信装置。

【請求項 3】 請求項 1 の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を通信路を通じて受信する暗号鍵受信手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された前記情報を復号する復号手段とを有する情報受信装置。

【請求項 4】 前記暗号鍵受信手段は、新しい暗号鍵が得られるまで古い暗号鍵を保持する請求項 3 記載の情報受信装置。

【請求項 5】 請求項 2 の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された情報を復号する復号手段とを有する情報受信装置。

【請求項 6】 前記照合情報は前記暗号鍵の有効期間の情報を含み、該有効期間の情報に基づいて前記情報配信装置との通信路の接続／切断を行なう通信路制御手段を有する、請求項 5 記載の情報受信装置。

【請求項 7】 請求項 2 の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された前記情報に関する関連情報と前記照合情報を得て両者を照合し、復号が許可された場合のみ前記照合情報を出力する照合情報出力手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された情報を復号する復号手段とを有する情報受信装置。

【請求項 8】 請求項 2 の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む前記照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された前記情報を含む情報から暗号化された前記情報に関する関連情報を分離する関連情報分離手段と、前記関連情報と前記照合情報を得て両者を照

合し、復号が許可された場合のみ前記照合情報を出力する照合情報出力手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された前記情報を復号する復号手段とを有する情報受信装置。

【請求項 9】 前記関連情報は、暗号化された情報の情報識別子を含み、前記照合情報は、復号できる情報の情報識別子を一つ以上含み、前記照合情報出力手段は前記照合情報に含まれる情報識別子の中に、前記関連情報に含まれる情報識別子が含まれていることを、前記照合情報を出力する条件とする請求項 8 記載の情報受信装置。

【請求項 10】 前記関連情報は、暗号化された情報の秘匿度を表す数値を含み、前記照合情報は、復号できる情報の秘匿度を表す数値を含み、前記照合情報出力手段は前記関連情報に含まれる秘匿度が、前記照合情報に含まれる秘匿度以下であることを、前記照合情報を出力する条件とする請求項 8 記載の情報受信装置。

【請求項 11】 前記関連情報は、暗号の復号方法を指示する情報を含み、前記照合情報出力手段は前記関連情報に含まれる暗号の復号方法に従い前記照合情報受信手段を制御して照合情報を取得する請求項 8 記載の情報受信装置。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、情報を暗号化して不特定多数に対して放送し、受信者のみが受信した暗号化された情報を復号する情報配信・受信システムに関する。

**【0002】**

【従来の技術】放送において受信者を限定したい場合、放送内容を暗号化して暗号鍵を持つものだけが暗号を復号して放送内容を知ることができるようにするのが一般的である。たとえば、有料放送では放送内容を暗号化し、受信料を支払う受信者のみが暗号を復号することができるようにする必要がある。これを実現するため、従来は復号装置に付加するハードウェアを用意しこれに暗号鍵を記録したものか、あるいは復号装置の一部もしくは全体を、暗号を復号する権利のある者に提供する方法が採られていた。

【0003】また、有料放送のように「見た分だけ課金する」ことが必要な場合は、復号操作を行ったことに対する課金処理、または復号を行った際の料金徴収者への通知を自動的に行えることが望ましい。このため、暗号を復号する装置においては、暗号が復号される条件を情報提供者の側で制御することができるか、あるいは暗号が復号されたことを確実に情報提供者に伝えることができる装置が要求される。従来、この目的のためには復号操作を行ったことを IC カードなどのハードウェアに記録し、この記録を情報提供者が定期的に回収することで課金等を行っていた。

## 【0004】

【発明が解決しようとする課題】これらの方法は、復号装置や暗号鍵の複製により、復号する権利のない者が復号を行う可能性や、ICカードに記録されたデータを改変され、正常に課金が行えない可能性があった。また、ICカードその他の付加的なハードウェアに対するコスト、復号操作を行った記録を回収するコスト等がかかり、有料情報提供サービスのコストアップの原因となっていた。

【0005】本発明の目的は、暗号化された情報を多数の利用者に同時に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険が小さい情報配信装置および情報受信装置を提供することにある。

## 【0006】

【課題を解決するための手段】本発明の第1の情報配信装置は、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された情報を含む情報を放送する放送送信手段と、暗号鍵を通信路を通じて送信する暗号鍵送信手段とを有する。また、本発明の第1の情報受信装置は、放送された情報を含む情報を受信する放送受信手段と、暗号鍵を通信路を通じて受信する暗号鍵受信手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0007】このシステムでは利用者は暗号と暗号鍵を常に受信しているので、送信側では任意の時刻に暗号鍵を変更することができる。したがって、多数の利用者へ暗号を放送することにより情報配信を行う際に、暗号鍵の複製や不正使用が行われる危険を小さくすることができる。

【0008】本発明の実施態様によれば、暗号鍵受信手段は、新しい暗号鍵が得られるまで古い暗号鍵を保持する。

【0009】回線断後も暗号鍵を保持することができるので、通信回線を切断しても次に暗号鍵が変化するまでは復号を続けることができる。通信回線として電話回線を使用する場合は、通信料金削減の点から、この装置が有用である。

【0010】本発明の第2の情報配信装置は、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された情報を含む情報を放送する放送送信手段と、暗号鍵を含む照合情報を通信路を通じて送信する照合情報送信手段とを有する。本発明の第2の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0011】本発明の実施態様によれば、情報受信装置は、照合情報が暗号鍵の有効期間の情報を含み、該有効期間の情報に基づいて情報配信装置との通信路の接続／

切断を行なう通信路制御手段を有する。これによりシステムの運用上の利便性が高まる。

【0012】本発明の第3の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された情報に関する関連情報と照合情報を得て両者を照合し、復号が許可された場合のみ照合情報を出力する照合情報出力手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0013】あらかじめ正しい関連情報を受信者が入手している場合に限り復号を行うことができるので、情報の受信者をより限定することができる。

【0014】本発明の第4の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された情報を含む情報から暗号化されている情報に関する関連情報を分離する関連情報分離手段と、関連情報と照合情報を得て両者を照合し、復号が許可された場合のみ照合情報を出力する照合情報出力手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0015】本発明の実施態様によれば、関連情報は、暗号化されている情報の情報識別子を含み、照合情報は、復号できる情報の情報識別子の一つ以上を含み、照合情報出力手段は照合情報に含まれる情報識別子の中に、関連情報に含まれる情報識別子が含まれていることを、照合情報を出力する条件とする。

【0016】本発明の実施態様によれば、関連情報は、暗号化されている情報の秘匿度を表す数値を含み、照合情報は、復号できる情報の秘匿度を表す数値を含み、照合情報出力手段は関連情報に含まれる秘匿度が、照合情報に含まれる秘匿度以下であることを、照合情報を出力する条件とする。

【0017】暗号が暗号鍵に対応するものであるかどうかを復号を行わずに試験することができる。

【0018】本発明の実施態様によれば、関連情報は、暗号の復号方法を指示する情報を含み、照合情報出力手段は関連情報に含まれる暗号の復号方法に従い照合情報受信手段を制御して照合情報を取得する。

【0019】照合情報の請求先が複数存在する場合でも、暗号に対応した適切な照合情報を取得することができる。

## 【0020】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0021】図1は本発明の第1の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0022】暗号生成手段である暗号生成部101は送信情報と暗号鍵を受け取り、送信情報を暗号化して出力する。放送送信手段である放送送信部102は暗号化された情報を受け取り、不特定多数に対して放送する。暗号鍵送信手段を含むセンタ側通信部103は暗号鍵を受け取り、通信路を通じて送信する。暗号鍵受信手段を含む端末側通信部104は通信路を通じて暗号鍵を受け取り、出力する。放送受信手段である放送受信部105は放送された暗号化された情報を受信し、出力する。復号手段である復号部106は暗号化された情報と暗号鍵を受け取り、復号済み情報を出力するが、暗号鍵が入力されない場合は動作を行わない。ここで、暗号生成部101と放送送信部102とセンタ側通信部103は情報配信装置を構成し、放送受信部105と端末側通信部104と復号部106は情報受信装置を構成している。

【0023】したがって、図1のシステムでは通信を行って暗号鍵を受信してる間だけ復号部106が動作する。

【0024】このシステムでは、その時点で送信される暗号と対応しているかぎりにおいて、暗号鍵を任意の時間に変化させてよい。したがって、受信側では情報を復号する必要がある間、常に通信路を通じて暗号鍵を受け取り続ける必要がある。

【0025】なお、通信路としては、端末側からセンタ側へ情報を送る必要はないので、一般的な双方向通信サービスのほか、同報通信サービスを利用することができる。

【0026】また、通信路として、電話網のように受信者が受信していることを交換機等の通信網上の装置で確認し記録することができる通信サービスを利用する場合には、受信者が暗号鍵を受信したことを確認できる。したがって、情報に対して課金する際に、通信履歴に基づいて課金額を決定することができる。

【0027】図2は本発明の第2の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0028】暗号生成手段である情報サーバ201は送信したい情報を受け取って暗号化し、放送送信手段である送信装置202を通じて放送用衛星に向けて送信する。また同時に、暗号鍵を暗号鍵送信手段であるモデム203を通じて専用線による通信路へ送出する。放送受信手段である受信装置205は衛星からの電波を受信し、暗号化された情報を出力する。同時に、暗号鍵受信手段であるモデム204は通信路から暗号鍵を受信し、出力する。復号手段である復号部206は暗号化された情報を暗号鍵を用いて解読し、復号済み情報を出力する。ここで、情報サーバ201と送信装置202とモデム203は情報配信装置を構成し、モデム204と受信装置205と復号部206は情報受信装置を構成している。

【0029】情報サーバ201は任意の時間に暗号鍵を変更する。したがって、暗号を持続的に復号することができるのは通信路に接続されている情報受信装置のみとなる。

【0030】以上の説明では通信路として専用線を想定したが、通常の電話回線やCATV回線も使用可能である。

【0031】なお、端末側通信部105、モデム204は、回線断後も暗号鍵を保持するようにしてもよい。この場合、通信回線を切断しても次に暗号鍵が変化するまでは復号を続けることができる。通信回線として電話回線を使用する場合は、通信料金削減の点から、有用である。

【0032】図3は本発明の第3の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0033】暗号生成部301、放送送信部302、放送受信部305、復号部308の機能はそれぞれ図1中の暗号生成部101、放送送信部102、放送受信部105、復号部106の機能と同様である。

【0034】照合情報生成部303は暗号鍵を受け取り、暗号鍵に任意の情報を付加した照合情報を生成し、出力する。照合情報送信手段であるセンタ側通信部304は照合情報を受け取り、通信路を通じて送信する。照合情報受信手段である端末側通信部306は通信路を通じて照合情報を受け取り、出力する。暗号鍵分離手段である暗号鍵抽出部307は照合情報を受け取り、暗号鍵を抽出して出力する。ここで暗号生成部301、放送送信部302、照合情報生成部303、センタ側通信部304は情報配信装置を構成し、放送受信部305、端末側通信部306、暗号鍵抽出部307、復号部308は情報受信装置を構成している。

【0035】本システムでは、暗号鍵に関する付加情報を照合情報に含めて通信する。付加情報としては暗号鍵が作成された時刻、暗号鍵の有効期間、復号アルゴリズム識別子、放送サービスのサービス識別子、サービス提供者識別子などを用いることができる。端末側通信部306が照合情報を保持できる場合は、照合情報の中に例えば暗号鍵の有効期間を含めておき、受信側の通信路制御手段でこれを参照して暗号鍵の有効期間が切れるまでは通信回線を切断しておくことができる。

【0036】図4は本発明の第4の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0037】暗号生成部401、放送送信部402、照合情報生成部403、センタ側通信部404、端末側通信部406、暗号鍵抽出部408、放送受信部405、復号部409の機能はそれぞれ図3中の暗号生成部301、放送送信部302、照合情報生成部303、センタ側通信部304、端末側通信部306、暗号鍵抽出部307、放送受信部305、復号部308の機能と同様である。

【0038】照合情報出力手段である照合部407は関連情報と照合情報を受け取り、照合情報と関連情報を比較して復号が許可される場合のみ照合情報を出力する。

【0039】ここで、暗号生成部401、放送送信部402、照合情報生成部403、センタ側通信部404は情報配信装置を構成し、放送受信部405、端末側通信部406、照合部407、暗号鍵抽出部408、復号部409は情報受信装置を構成している。

【0040】照合情報と関連情報は暗号化されている情報の復号を許可するか否かにかかわる情報を用いることができる。たとえば照合情報で送られたパスワードと関連情報で入力されたパスワードが一致した場合のみ復号を許可するという使い方が可能である。この場合は、一般に行われているように、照合情報で送信するパスワードは逆変換が不可能な演算をあらかじめ施してから送信し、関連情報に対して同じ演算を行った結果と比較すれば、照合情報の中からパスワードを盗まれる危険はない。

【0041】図1から図3のシステムでは通信回線に接続できれば必ず暗号を復号することができるが、図4のシステムではあらかじめ正しい関連情報を受信者が入手している場合に限り復号を行うことができるので、情報の受信者をより限定することができる。

【0042】図5は本発明の第5の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0043】暗号生成部501、照合情報生成部503、センタ側通信部504、端末側通信部505、暗号鍵抽出部509、復号部510の機能は図4中のそれぞれ暗号生成部401、照合情報生成部403、センタ側通信部404、端末側通信部406、暗号鍵抽出部408、復号部409の機能と同様である。

【0044】放送送信手段である放送送信部502は暗号化された情報と関連情報を受け取り、両者を含む放送信号を生成し、不特定多数に対して放送する。放送受信手段である放送受信部506は放送信号を受信し出力する。関連情報分離手段である関連情報分離部507は放送信号を受け取り、暗号と関連情報を抽出して出力する。照合情報出力手段である照合部508は関連情報と照合情報を比較し、比較結果により復号が許可される場合のみ照合情報を出力する。

【0045】ここで、暗号生成部501、放送送信部502、照合情報生成部503、センタ側通信部504は情報配信装置を構成し、端末側通信部505、放送通信部506、関連情報分離部507、照合部508、暗号抽出部509、復号部510は情報受信装置を構成している。

【0046】関連情報は暗号化されている情報に関する情報である。たとえば暗号に含まれている情報を表す情報識別子、情報の秘匿度を表す数値などである。一方、照合情報は暗号鍵の他に、関連情報と対応する復号許可

情報を含む。復号許可情報は暗号鍵が用いられる条件を記述した情報である。例としては、一つまたは複数の情報を表す情報識別子や復号できる情報の秘匿度を表す数値などである。

【0047】照合情報生成部503を複数用いてそれぞれ異なる情報識別子や情報秘匿度を含む照合情報を生成し、異なる通信チャネルを用いて送信すれば、受信側が復号できる情報を、どの通信チャネルに接続するかにより決定することができる。

【0048】図6は本発明の第6の実施形態の情報配信・受信システムの構成を示すブロック図である。このシステムはCS放送においてスクランブル暗号化されたMPEG2パケットの暗号鍵を通信路を通じて取得する。ここでは通信路として電話回線を想定する。また、このシステムでは放送番組と共にその番組の種類に関する情報が放送される。一方、通信路では暗号鍵のほかはその暗号鍵を使用できる番組の種類を送信する。受信側では、この番組の種類に従って、暗号を復号するか否かを決定する。

【0049】タイマ601は一定時間毎に暗号鍵更新要求を出力する。暗号鍵生成部602は暗号鍵更新要求を受けると新しい暗号鍵を生成し出力する。照合情報生成部605は暗号鍵に許可する番組の種類を付加して出力する。図7は照合情報に用いる番組の種類に関する情報の一例を示す図である。生成された照合情報はモデム606を通じて通信路へ送信される。照合情報は、一つのセンタから複数の利用者へ送信する必要があるため、同報型の通信サービスを利用する。暗号生成手段である暗号生成部603は暗号鍵とMPEG符号を受け取り暗号を生成して出力する。放送送信手段であるCS放送装置604は関連情報と暗号を受け取り、放送パケットとして衛星を通じて放送する。関連情報には図7と同じ形式で現在放送中の番組のジャンルを示す情報が含まれる。放送受信手段であるCS受信装置608は衛星からの放送を受信し放送パケットを出力する。関連情報分離手段である関連情報分離部611は放送パケットを受け取り、関連情報と暗号を分離し、出力する。受信側モデム607は照合情報を通信路から受信し出力する。照合情報出力手段である照合部609は照合情報と関連情報を受け取り、関連情報中の番組ジャンルが照合情報中の番組ジャンルに含まれていれば照合情報を出力する。暗号鍵分離手段である暗号鍵抽出部610は照合情報から暗号鍵を抽出し出力する。復号手段である復号部612は暗号と暗号鍵を受け取り、暗号を復号して得られるMPEG符号を出力する。

【0050】ここで、タイマ601、鍵生成部602、暗号生成部603、CS放送装置604、照合情報生成部605、モデム606は情報配信装置を構成し、モデム607、CS受信装置608、照合部609、暗号鍵抽出部610、関連情報分離部611、復号部612は

情報受信装置を構成している。

【0051】以上の説明では関連情報と照合情報には番組のジャンルに関する情報を持たせたが、ジャンル以外の情報を持たせることもできる。図8は関連情報に番組識別子、照合情報に複数の番組識別子のリストを持たせ、リストに示された番組のみ復号可とする例である。また、図9は関連情報には番組のレベル、照合情報にはその照合情報で復号を許可する番組のレベルを持たせ、そのレベル以下の番組のみ復号可とする例である。

【0052】また、図6において関連情報の中に照合情報を入力する際に必要な同報型通信サービスの電話番号を含めておけば、モデム607をこの電話番号に対して発呼するよう制御することにより、照合情報の入手先が目的に応じて複数存在しても、自動的に照合情報を取得することができる。

【0053】

【発明の効果】以上説明したように、本発明は、下記のような効果がある。

(1) 請求項1と3の発明は、暗号の復号に必要な暗号鍵を頻繁に変更することができるので、暗号化された情報を多数の利用者に同時に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険が小さい。

【0054】また、通信路として、電話網のように受信者が受信していることを交換機等の通信網上の装置で確認し記録することができる場合には、受信者が暗号鍵を受信したことを確認できるので、情報に対して課金する際に、通信履歴に基づいて課金額を決定することができる。これは有料放送をスクランブラ／デスクランブラを用いて行う際に、見た分だけ課金することを可能にする。

(2) 請求項4の発明は、請求項1と3からなるシステムの機能を短い通信時間で実現することができる。

(3) 請求項2と5と6の発明は、暗号鍵の有効期間など付加的な情報を通信することにより、装置の運用上の利便性を高めることができる。

(4) 請求項2と7の発明は、復号を行う際に、復号を行う者が正しい利用者かどうかを受信者の側で試験することができる。

(5) 請求項8、9、10の発明は、暗号が暗号鍵に対応するものであるかどうかを復号を行わずに試験することができる。この機能は、ある特定の情報を、特定の受信者集合に対して、復号を許可するかどうかを送信側で指定するために用いることができる。たとえば有料放送で、ある一定の課金額の通信チャンネルを通じて暗号鍵を取得している利用者が、どの番組を視聴することができるかを指定することができる。

(6) 請求項11の発明は、照合情報の請求先が複数存在する場合でも、暗号に対応した適切な照合情報を取得することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図2】本発明の第2の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図3】本発明の第3の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図4】本発明の第4の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図5】本発明の第5の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図6】本発明の第6の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図7】本発明の第5、第6の実施形態において照合情報に含まれる情報の例を示す図である。

【図8】本発明の第5、第6の実施形態において照合情報に含まれる情報および照合部の動作の一例を示す図である。

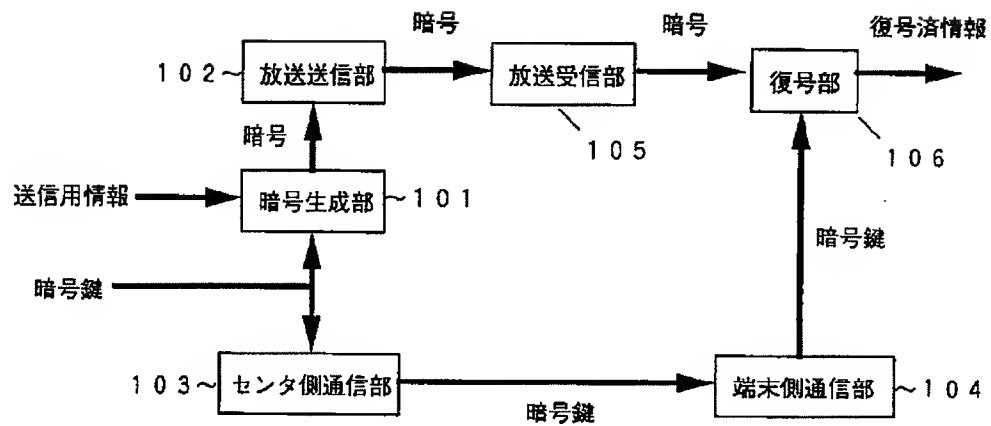
【図9】本発明の第5、第6の実施形態において照合情報に含まれる情報および照合部の動作の一例を示す図である。

【符号の説明】

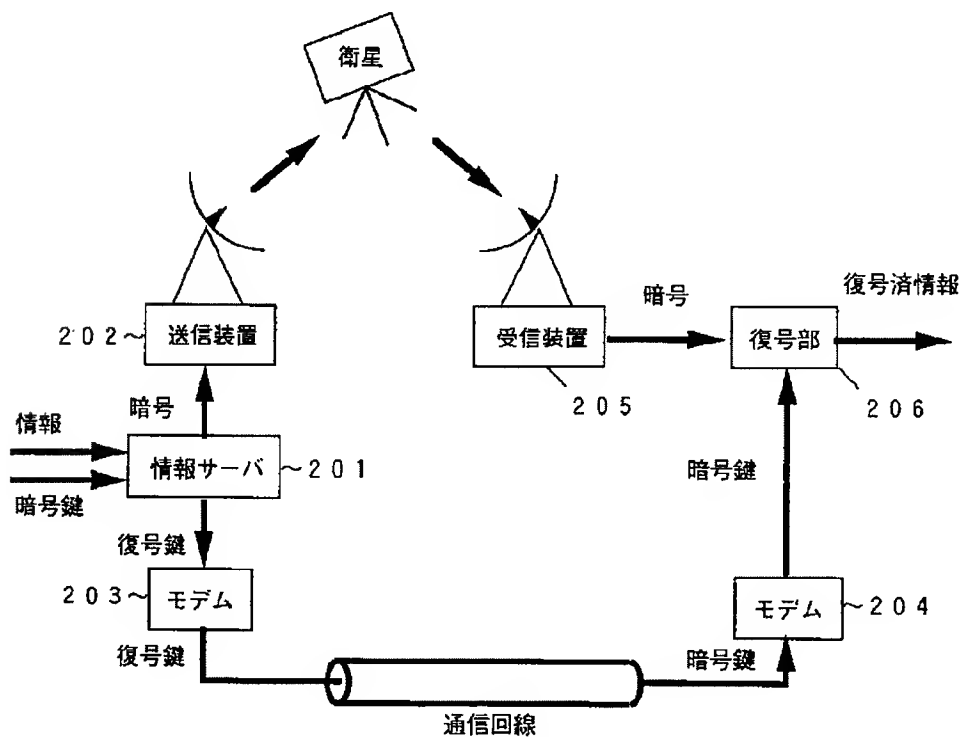
101	暗号生成部
102	放送送信部
103	センタ側通信部
104	端末側通信部
105	放送受信部
106	復号部
201	情報サーバ
202	送信装置
203	モデム
204	モデム
205	受信装置
206	復号装置
301	暗号生成部
302	放送送信部
303	照合情報生成部
304	センタ側通信部
305	放送受信部
306	端末側通信部
307	暗号鍵抽出部
308	復号部
401	暗号生成部
402	放送送信部
403	照合情報生成部
404	センタ側通信部
405	放送受信部
406	端末側通信部
407	照合部
408	暗号鍵抽出部
409	復号部

501	暗号生成部	602	暗号鍵生成部
502	放送送信部	603	暗号生成部
503	照合情報生成部	604	CS放送装置
504	センタ側通信部	605	照合情報生成部
505	端末側通信部	606	モデム
506	放送受信部	607	モデム
507	関連情報分離部	608	CS受信装置
508	照合部	609	照合部
509	暗号鍵抽出部	610	暗号鍵抽出部
510	復号部	611	関連情報分離部
601	タイマ	612	復号部

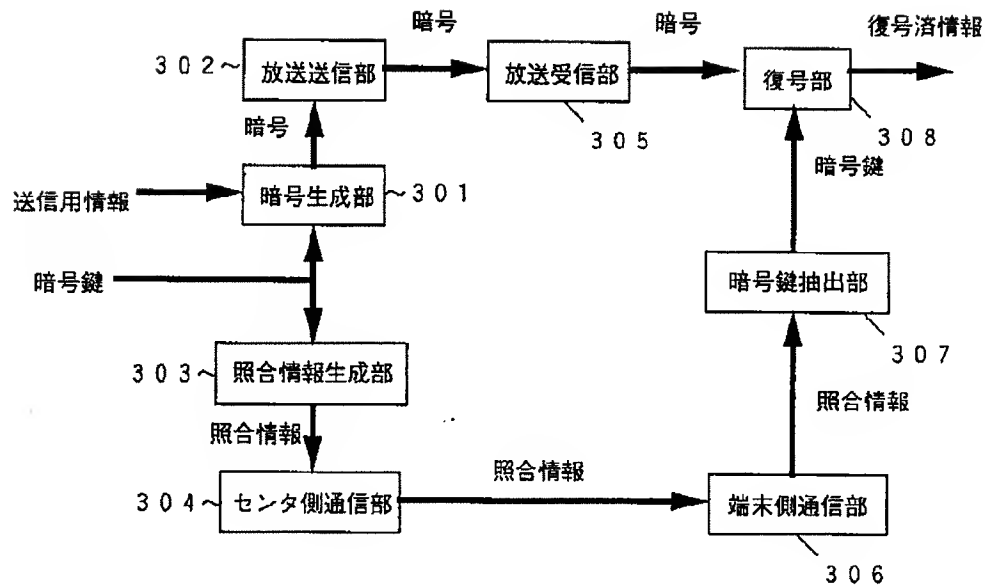
【図1】



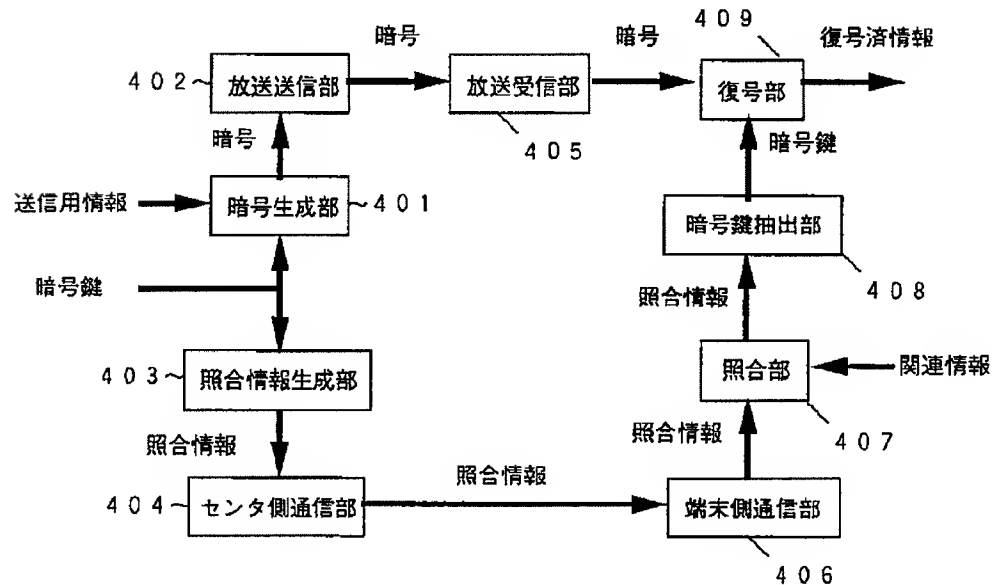
【図2】



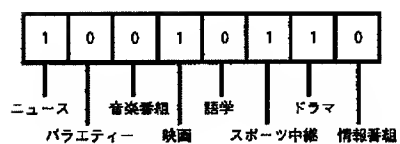
【図3】



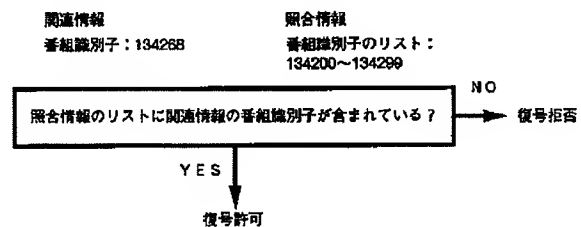
【図4】



【図7】

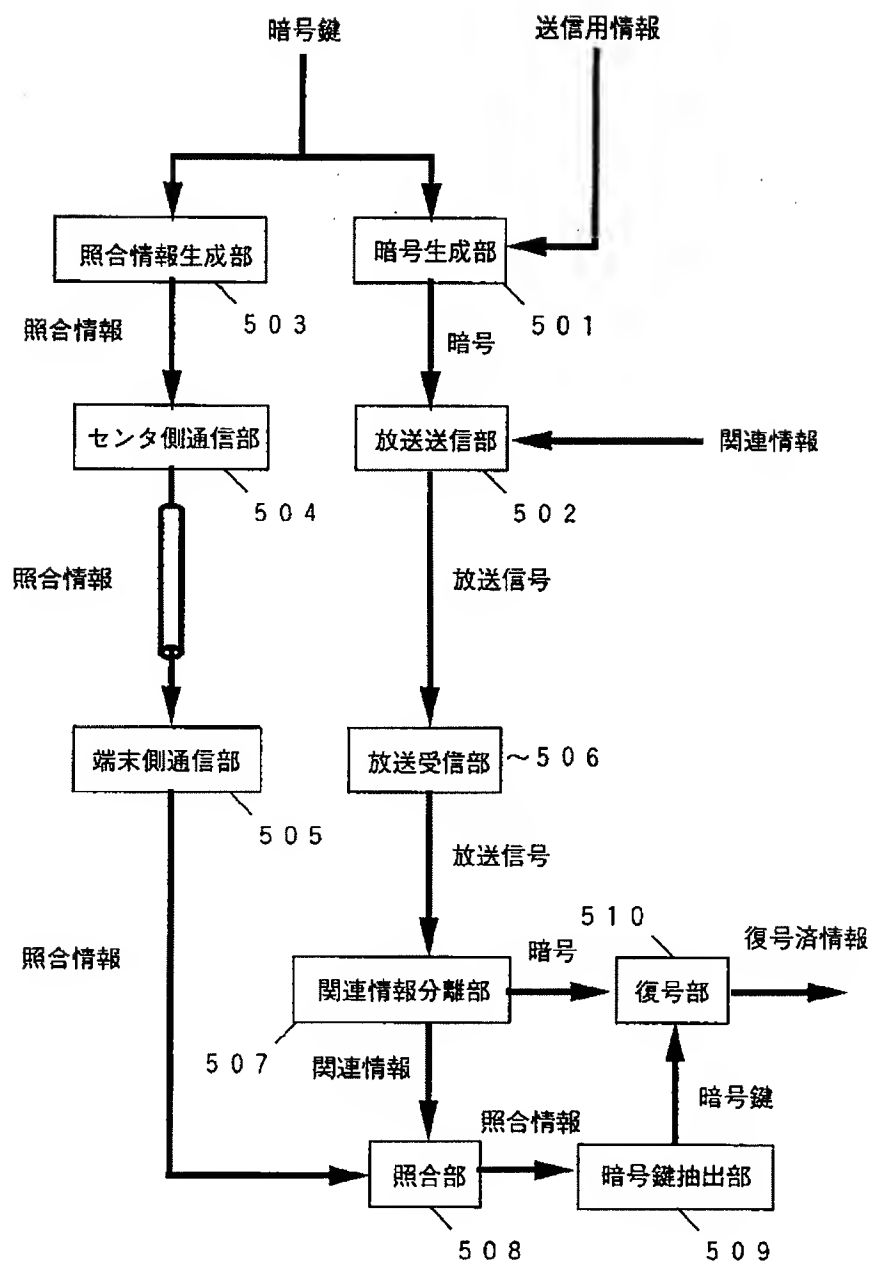


【図8】

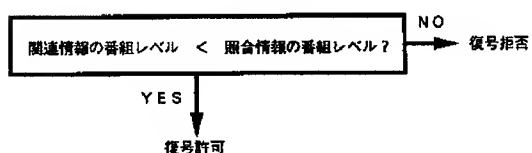




【図5】



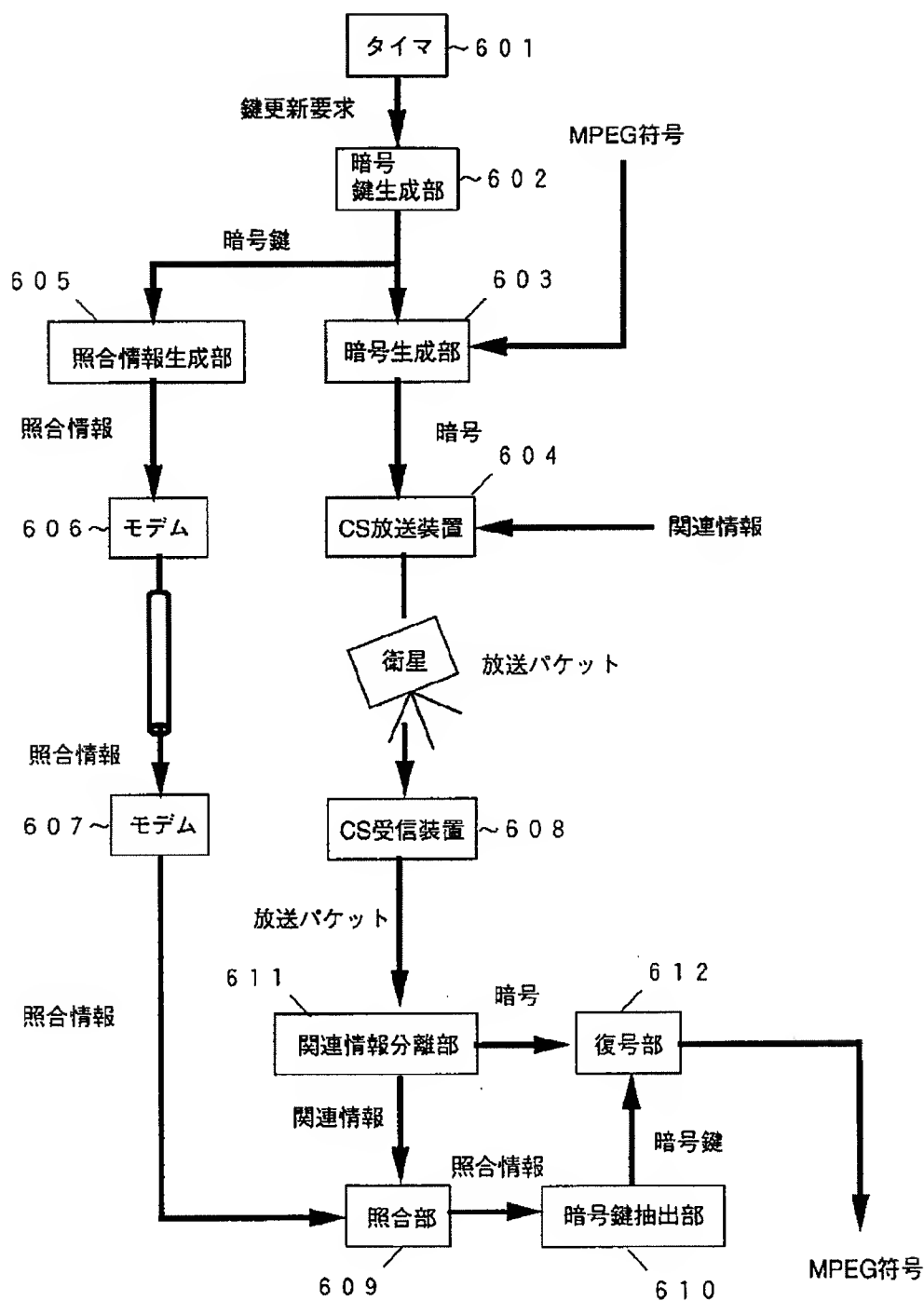
【図9】



## 番組レベルの例

- レベル1：映画、スポーツ中継、バラエティを除く全番組
- レベル2：映画、スポーツ中継を除く全番組
- レベル3：スポーツ中継を除く全番組
- レベル4：全番組

【図6】



フロントページの続き

(72)発明者 鈴木 達郎  
東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 熊谷 佳子  
東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-117173

(43)Date of publication of application : 06.05.1998

---

(51)Int.Cl. H04H 1/00  
H04K 1/00  
H04N 7/16  
H04N 7/167

---

(21)Application number : 08-269938 (71)Applicant : NIPPON TELEGR & TELEPH  
CORP <NTT>

(22)Date of filing : 11.10.1996 (72)Inventor : HAYAKAWA KAZUHIRO  
FUKUNAGA HIRONOBU  
WATABE TOMOKI  
SUZUKI TATSURO  
KUMAGAI YOSHIKO

---

## (54) INFORMATION DISTRIBUTER AND INFORMATION RECEIVER

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To lessen the danger that an illegal user decodes encrypted information or copies an encryption key in the case that encrypted information is distributed to a large number of users.

**SOLUTION:** An encryption generating section 101 receives transmission information and an encryption key and encrypts the transmission information and provides an output of the result. A broadcast transmission section 102 receives the encrypted information and broadcasts the information to a large number of unspecified persons. A center side communication section 104 receives the encryption key and sends it to a communication channel. A terminal equipment side communication section 104 receives the encryption key through the communication channel and provides an output of it. A broadcast reception section 105 receives the broadcast encrypted information and provides an output of it. A decoding section 106 receives the encrypted information and the encryption key and provides an output of decoded information but is not operative when the section 106 receives no encryption key.

---

## CLAIMS

---

[Claim(s)]

[Claim 1]An information distributing device which enciphers and distributes

information comprising:

A cipher generation means which obtains information and an encryption key and enciphers said information.

A broadcast transmitting means which broadcasts information including said enciphered information.

An encryption key transmitting means which transmits said encryption key through a channel.

[Claim 2] An information distributing device which enciphers and distributes information comprising:

A cipher generation means which obtains information and an encryption key and enciphers said information.

A broadcast transmitting means which broadcasts information including said enciphered information.

A collation information transmitting means which transmits collation information containing said encryption key through a channel.

[Claim 3] An information reception device which receives information enciphered with an information distributing device of claim 1 comprising:

A broadcast receiving means which receives information including enciphered information.

An encryption key reception means which receives said encryption key through a channel.

A decoding means which decodes said information which obtained said enciphered information and said encryption key and was enciphered.

[Claim 4] The information reception device according to claim 3 which holds an old encryption key until an encryption key with said new encryption key reception means is obtained.

[Claim 5] An information reception device which receives information enciphered with an information distributing device of claim 2 comprising:

A broadcast receiving means which receives information including enciphered information.

A collation information reception means which receives collation information containing said encryption key through a channel.

Encryption key separating mechanism which separates said encryption key from said collation information.

A decoding means which decodes information which obtained said enciphered information and said encryption key and was enciphered.

[Claim 6] The information reception device according to claim 5 with which said collation information has a channel control means which performs connection/cutting of a channel with said information distributing device based on information on this shelf-life including information on a shelf-life of said encryption

key.

[Claim 7]An information reception device which receives information enciphered with an information distributing device of claim 2comprising:

A broadcast receiving means which receives information including enciphered information.

A collation information reception means which receives collation information containing said encryption key through a channel.

A collation information output means which outputs said collation information only when pertinent information about said enciphered information and said collation information are acquiredboth are compared and decoding is permitted.

Encryption key separating mechanism which separates said encryption key from said collation informationand a decoding means which decodes information which obtained said enciphered information and said encryption keyand was enciphered.

[Claim 8]An information reception device which receives information enciphered with an information distributing device of claim 2comprising:

A broadcast receiving means which receives information including enciphered information.

A collation information reception means which receives said collation information containing said encryption key through a channel.

Pertinent information separating mechanism which separates pertinent information about said information enciphered from information including said enciphered information.

A collation information output means which outputs said collation information only when said pertinent information and said collation information are acquiredboth are compared and decoding is permittedencryption key separating mechanism which separates said encryption key from said collation informationand a decoding means which decodes said information which obtained said enciphered information and said encryption keyand was enciphered.

[Claim 9]Said pertinent information including an information identifier of enciphered information said collation informationThe information reception device according to claim 8 which makes it conditions which output said collation information to include one or more information identifiers of information which can be decodedand to contain an information identifier contained in said pertinent information in an information identifier by which said collation information output means is included in said collation information.

[Claim 10]Said pertinent information the degree of secrecy of enciphered information including a numerical value to express said collation informationThe information reception device according to claim 8 which includes a numerical value showing the degree of secrecy of information which can be decodedand makes it conditions which output said collation information for said collation information output means to be below the degree of secrecy by which the degree of secrecy contained in said pertinent information is contained in said collation information.

[Claim 11]The information reception device according to claim 8 which said pertinent information includes information which directs a decoding method of a codeand said collation information output means controls said collation information reception means in accordance with a decoding method of a code contained in said pertinent informationand acquires collation information.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention enciphers informationbroadcasts it to many and unspecified personsand relates to the information distribution receiving system which decodes the enciphered information which only the addressee received.

[0002]

[Description of the Prior Art]It is common only for what enciphers contents of broadcast and has an encryption key to decode a codeand to enable it to get to know contents of broadcast to limit an addressee in broadcast. For examplecontents of broadcast are enciphered and only the addressee who pays a subscription fee needs to enable it to decode a code in paid broadcasting. In order to realize thisor it would not prepare conventionally the hardware added to a decoding device and would not record an encryption key on thisthe method of providing with some or the whole of a decoding device a person with the right to decode a code was taken.

[0003]When what "only a part to have seen is charged for" like paid broadcasting is requiredit is desirable that a notice to the rate collection person at the time of performing accounting to having performed decoding operation or decoding can be performed automatically. For this reasonin the device which decodes a codethe device which can tell an information provider certainly that could control the conditions by which a code is decoded by the information provider sideor the code was decoded is required. It recorded having performed decoding operation conventionally for this purpose on hardwaressuch as an IC cardand fee collection etc. were performed because an information provider collects these records periodically.

[0004]

[Problem(s) to be Solved by the Invention]These methods had a possibility that a person without the right to decode will decode by the duplicate of a decoding device or an encryption keyand the data recorded on the IC card changedand may be unable to be charged normally. The cost to the hardware in which others are [ being an IC card and ] additionalthe cost which collects the records which performed decoding operationetc. startedand it had become a cause of the cost hike of pay information providing service.

[0005]When the purpose of this invention distributes the enciphered information to

many users simultaneously there is a risk of an inaccurate user decoding or reproducing an encryption key in providing a small information distributing device and an information reception device.

[0006]

[Means for Solving the Problem] The 1st information distributing device of this invention is provided with the following.

A cipher generation means which obtains information and an encryption key and enciphers said information.

A broadcast transmitting means which broadcasts information including enciphered information.

An encryption key transmitting means which transmits an encryption key through a channel.

The 1st information reception device of this invention is provided with the following.

A broadcast receiving means which receives information including broadcast information.

An encryption key reception means which receives an encryption key through a channel.

A decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.

[0007] In this system since a user has always received a code and an encryption key he can change an encryption key at arbitrary time in the transmitting side. Therefore when performing distribute information by broadcasting a code to many users a risk of a duplicate and an unauthorized use of an encryption key being performed can be made small.

[0008] According to the embodiment of this invention an encryption key reception means holds an old encryption key until a new encryption key is obtained.

[0009] Since after disconnection can hold an encryption key it can continue decoding until an encryption key changes next even if it cuts a communication line. When using a telephone line as a communication line a point of telex rate gold reduction to this device is useful.

[0010] The 2nd information distributing device of this invention is provided with the following.

A cipher generation means which obtains information and an encryption key and enciphers said information.

A broadcast transmitting means which broadcasts information including enciphered information.

A collation information transmitting means which transmits collation information containing an encryption key through a channel.

The 2nd information reception device of this invention is provided with the following.

A broadcast receiving means which receives information including enciphered information.

A collation information reception means which receives collation information containing an encryption key through a channel.

Encryption key separating mechanism which separates an encryption key from collation information.

A decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.

[0011]As for an information reception device according to the embodiment of this invention collation information has a channel control means which performs connection/cutting of a channel with an information distributing device based on information on this shelf-life including information on a shelf-life of an encryption key. Thereby convenience on employment of a system increases.

[0012]The 3rd information reception device of this invention is provided with the following.

A broadcast receiving means which receives information including enciphered information.

A collation information reception means which receives collation information containing an encryption key through a channel.

A collation information output means which outputs collation information only when pertinent information and collation information about enciphered information are acquired both are compared and decoding is permitted.

Encryption key separating mechanism which separates an encryption key from collation information and a decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.

[0013]Since it can restrict when an addressee has obtained right pertinent information beforehand and it can decode an addressee of information can be limited more.

[0014]The 4th information reception device of this invention is provided with the following.

A broadcast receiving means which receives information including enciphered information.

A collation information reception means which receives collation information containing an encryption key through a channel.

Pertinent information separating mechanism which separates pertinent information about information enciphered from information including enciphered information.

A collation information output means which outputs collation information only when pertinent information and collation information are acquired both are compared and decoding is permitted encryption key separating mechanism which separates an encryption key from collation information and a decoding means which decodes information which obtained information and an encryption key which were enciphered and was enciphered.



[0015]According to the embodiment of this inventionpertinent information including an information identifier of information enciphered collation informationOne or more information identifiers of information which can be decoded are includedand a collation information output means makes it conditions which output collation information to contain an information identifier contained in pertinent information in an information identifier contained in collation information.

[0016]According to the embodiment of this inventionpertinent information the degree of secrecy of information enciphered including a numerical value to express collation informationIncluding a numerical value showing the degree of secrecy of information which can be decodeda collation information output means makes it conditions which output collation information for the degree of secrecy contained in pertinent information to be below the degree of secrecy contained in collation information.

[0017]It can examine without whether a code is a thing corresponding to an encryption keyand decoding.

[0018]According to the embodiment of this inventionpertinent information includes information which directs a decoding method of a codeand a collation information output means controls a collation information reception means in accordance with a decoding method of a code contained in pertinent informationand acquires collation information.

[0019]Even when two or more billing addresses of collation information existsuitable collation information corresponding to a code can be acquired.

[0020]

[Embodiment of the Invention]Nextan embodiment of the invention is described with reference to drawings.

[0021]Drawing 1 is a block diagram showing the composition of the information distribution receiving system of a 1st embodiment of this invention.

[0022]The code generation part 101 which is a cipher generation means receives the information for transmissionand an encryption keyand enciphers and outputs the information for transmission. The broadcast transmission section 102 which is a broadcast transmitting means receives the enciphered informationand broadcasts to many and unspecified persons. The center side communications department 103 including an encryption key transmitting means receives an encryption keyand transmits through a channel. The terminal side communications department 104 including an encryption key reception means receives and outputs an encryption key through a channel. The broadcast receive section 105 which is a broadcast receiving means receives and outputs the broadcast information which was enciphered. Although the decoding part 106 which is a decoding means receives the information and encryption key which were enciphered and the information that it decodes is outputtedit does not operatewhen an encryption key is not inputted. Herethe code generation part 101the broadcast transmission section 102and the center side communications department 103 constitute an information distributing deviceand the broadcast receive section 105the terminal side communications department 104and the decoding part 103 constitute the

information reception device.

[0023] Therefore in the system of drawing 1 only while communicating and having received the encryption key the decoding part 106 operates.

[0024] In this system as long as it corresponds with the code transmitted at that time an encryption key may be changed at arbitrary time. Therefore in a receiver while decoding information it is necessary to always continue receiving an encryption key through a channel.

[0025] Since it is not necessary to send information to the center side from the terminal side as a channel multiaddress calling besides a general interactive communications service can be used.

[0026] When using the communications service which can check and record that the addressee has received like a telephone network as a channel with the device on communications network such as a switchboard it can check that the addressee has received the encryption key. Therefore when charging to information charge amount can be determined based on a communication history.

[0027] Drawing 2 is a block diagram showing the composition of the information distribution receiving system of a 2nd embodiment of this invention.

[0028] The information server 201 which is a cipher generation means receives information to transmit ciphers and transmits towards the satellite for broadcast through the sending set 202 which is a broadcast transmitting means. An encryption key is simultaneously sent out to the channel by a dedicated line through the modem 203 which is an encryption key transmitting means. The receiving set 205 which is a broadcast receiving means receives the electric wave from a satellite and outputs the enciphered information. Simultaneously the modem 204 which is an encryption key reception means receives and outputs an encryption key from a channel. The decoding part 206 which is a decoding means decodes the enciphered information using an encryption key and outputs the information that it decodes. Here the information server 201 the sending set 202 and the modem 203 constitute an information distributing device and the modem 204 the receiving set 205 and the decoding part 206 constitute the information reception device.

[0029] The information server 201 changes an encryption key at arbitrary time. Therefore that a code can be decoded continuously becomes only the information reception device connected to the channel.

[0030] Although the dedicated line was assumed as a channel in the above explanation it is usable also in a usual telephone line and CATV circuit.

[0031] It may be made for the terminal side communications department 105 and the modem 204 to hold an encryption key even after disconnection. In this case decoding can be continued until an encryption key changes next even if it cuts a communication line. When using a telephone line as a communication line it is useful from a point of telex rate gold reduction.

[0032] Drawing 3 is a block diagram showing the composition of the information distribution receiving system of a 3rd embodiment of this invention.

[0033] The function of the code generation part 301 the broadcast transmission

section 302the broadcast receive section 305and the decoding part 308 is the same as the function of the code generation part 101 in drawing 1the broadcast transmission section 102the broadcast receive section 105and the decoding part 106 respectively.

[0034]The collation information generation part 303 receives an encryption keyand generates and outputs the collation information which added arbitrary information to the encryption key. The center side communications department 304 which is a collation information transmitting means receives collation informationand transmits through a channel. The terminal side communications department 306 which is a collation information reception means receives and outputs collation information through a channel. The encryption key extraction part 307 which is encryption key separating mechanism receives collation informationand extracts and outputs an encryption key. The code generation part 301the broadcast transmission section 302the collation information generation part 303and the center side communications department 304 constitute an information distributing device hereand the broadcast receive section 305the terminal side communications department 306the encryption key extraction part 307and the decoding part 308 constitute the information reception device.

[0035]In this systemthe additional information about an encryption key is included in collation informationand it communicates. As additional informationthe time when the encryption key was createdthe shelf-life of an encryption keya decoding algorithm identifierthe service identifier of broadcast servicea purveyor-of-service identifieretc. can be used. When the terminal side communications department 306 can hold collation informationthe shelf-life of the encryption key is included into collation informationand a communication line can be cut until the shelf-life of an encryption key goes out with reference to this by the channel control means of a receiver.

[0036]Drawing 4 is a block diagram showing the composition of the information distribution receiving system of a 4th embodiment of this invention.

[0037]The function of the code generation part 401the broadcast transmission section 402the collation information generation part 403the center side communications department 404the terminal side communications department 406the encryption key extraction part 408the broadcast receive section 405and the decoding part 409respectively The code generation part 301 in drawing 3the broadcast transmission section 302the collation information generation part 303It is the same as that of the function of the center side communications department 304the terminal side communications department 306the encryption key extraction part 307the broadcast receive section 305and the decoding part 308.

[0038]The collating part 407 which is a collation information output means receives pertinent information and collation informationand only when collation information is compared with pertinent information and decoding is permittedit outputs collation information.

[0039]Herethe code generation part 401the broadcast transmission section 402the \*\*\* information generating part 403and the center side communications

department 404 constitute an information distributing device and the broadcast receive section 405 the terminal side communications department 406 the collating part 407 the encryption key extraction part 408 and the decoding part 409 constitute the information reception device.

[0040] Collation information and the pertinent information can use the information in connection with whether decoding of the information enciphered is permitted. For example only when the password sent by collation information and the password entered by pertinent information are in agreement the usage of permitting decoding is possible. In this case the password which transmits by collation information transmits after performing beforehand the operation in which inverse transformation is impossible and if it compares with the result of having performed the same operation to pertinent information there will be no risk of a password being stolen out of collation information as generally carried out.

[0041] If connectable [ in the system of drawing 3 ] with a communication line from drawing 1a a code can certainly be decoded but since it can restrict when the addressee has obtained right pertinent information beforehand in the system of drawing 4 and it can decode the addressee of information can be limited more.

[0042] Drawing 5 is a block diagram showing the composition of the information distribution receiving system of a 5th embodiment of this invention.

[0043] The function of the code generation part 501 the collation information generation part 503 the center side communications department 504 the terminal side communications department 505 the encryption key extraction part 509 and the decoding part 510 each in drawing 4 The code generation part 401 the collation information generation part 403 the center side communications department 404 the terminal side communications department 406 the encryption key extraction part 408 It is the same as that of the function of the decoding part 409.

[0044] The broadcast transmission section 502 which is a broadcast transmitting means receives the information and pertinent information which were enciphered generates a broadcasting signal including both and broadcasts to many and unspecified persons. The broadcast receive section 506 which is a broadcast receiving means receives and outputs a broadcasting signal. The pertinent information separation part 507 which is pertinent information separating mechanism receives a broadcasting signal and extracts and outputs a code and pertinent information. The collating part 508 which is a collation information output means compares pertinent information with collation information and only when decoding is permitted by a comparison result it outputs collation information.

[0045] Here the code generation part 501 the broadcast transmission section 502 the collation information generation part 503 and the center side communications department 504 constitute an information distributing device and the terminal side communications department 505 the broadcast communication part 506 the pertinent information separation part 507 the collating part 508 the code extraction part 509 and the decoding part 510 constitute the information reception device.

[0046] Pertinent information is information about the information enciphered. For example they are an information identifier showing the information included in the

code a numerical value showing the degree of secrecy of information etc. On the other hand collation information includes decoding permit information [ other than an encryption key / pertinent information ]. Decoding permit information is information which describes the conditions for which an encryption key is used. It is a numerical value etc. which express as an example the degree of secrecy of the information identifier showing one or more information or the information which can be decoded.

[0047] If the collation information containing the information identifier from which each differs using the collation information generation part 503 two or more and the degree of information hiding is generated and it transmits using a different communications channel the information which can decode a receiver can be determined by with which communications channel it connects.

[0048] Drawing 6 is a block diagram showing the composition of the information distribution receiving system of a 6th embodiment of this invention. This system acquires the encryption key of the MPEG 2 packet by which scramble encryption was carried out in CS broadcasting through a channel. Here a telephone line is assumed as a channel. In this system the information about the kind of that program is broadcast with a program. On the other hand in a channel the kind of program which can use the encryption key other than an encryption key is transmitted. In a receiver it determines whether decode a code or not according to the kind of this program.

[0049] The timer 601 outputs an encryption key update request for every fixed time. The encryption key generation part 602 will generate and output a new encryption key if an encryption key update request is received. The collation information generation part 605 adds and outputs the kind of program permitted to an encryption key. Drawing 7 is a figure showing an example of the information about the kind of program used for collation information. The generated collation information is transmitted to a channel through the modem 606. Since it is necessary to transmit collation information to two or more users from one center multiple address type communications service is used. The code generation part 603 which is a cipher generation means receives an encryption key and MPEG numerals and generates and outputs a code. The CS broadcasting device 604 which is a broadcast transmitting means receives pertinent information and a code and broadcasts them through a satellite as a broadcast packet. The information which shows the genre of the program under present broadcast in the same form as drawing 7 is included in pertinent information. The CS receiving set 608 which is a broadcast receiving means receives the broadcast from a satellite and outputs a broadcast packet. The pertinent information separation part 611 which is pertinent information separating mechanism receives a broadcast packet and separates and outputs pertinent information and a code. The reception side modem 607 receives and outputs collation information from a channel. The collating part 609 which is a collation information output means receives collation information and pertinent information and if the program genre in pertinent information is contained in the program genre in collation information it will output

collation information. The encryption key extraction part 610 which is encryption key separating mechanism extracts and outputs an encryption key from collation information. The decoding part 612 which is a decoding means receives a code and an encryption key and outputs the MPEG numerals produced by decoding a code. [0050] The timer 601, the key generation part 602, the code generation part 603, the CS broadcasting device 604, the collation information generation part 605, and the modem 606 constitute an information distributing device here. The modem 607, the CS receiving set 608, the collating part 609, the encryption key extraction part 610, the pertinent information separation part 611, and the decoding part 612 constitute the information reception device.

[0051] Although the information about the genre of a program was given to pertinent information and collation information in the above explanation, information other than a genre can also be given. Drawing 8 is an example which makes possible [ decoding ] only the program which gave the list of two or more program identifiers to pertinent information at a program identifier and collation information, and was shown in the list. Drawing 9 is an example carried out to the level of a program with which the level of a program is permitted to pertinent information and it permits decoding to collation information by the collation information being given, and only the program below the level being decoded.

[0052] If the telephone number of required multiple address format \*\* service is included when collation information comes to hand in pertinent information in drawing 6, collation information is automatically acquirable even if two or more acquisition places of collation information exist according to the purpose by controlling to carry out call origination of the modem 607 to this telephone number.

[0053]

[Effect of the Invention] As explained above, this invention has the following effects.

(1) Since the invention of claims 1 and 3 can change an encryption key required for decoding of a code frequently when it distributes the enciphered information to many users simultaneously, its risk of an inaccurate user decoding or reproducing an encryption key is small.

[0054] Since it can check that the addressee has received the encryption key when it can be checked and recorded with the device on communications networks such as a switchboard that the addressee has received like a telephone network as a channel when charging to information, charge amount can be determined based on a communication history. When this performs paid broadcasting using a scrambler/descrambler, it makes it possible to charge only a part to have seen.

(2) The invention of claim 4 can realize the function of the system which consists of claims 1 and 3 by short hour corresponding.

(3) Claim 2 and the invention of 5 and 6 can improve the convenience on employment of a device by communicating additional information including the shelf-life of an encryption key, etc.

(4) When the invention of claims 2 and 7 decodes, it can examine by the addressee side whether those who decode are right users.

(5) The invention of claims 8 and 10 can be examined without whether a code is a thing corresponding to an encryption key and decoding. This function can use whether decoding is permitted for a certain specific information to a specific addressee set in order to specify at the transmitting side. For example the user who acquires the encryption key through the communications channel of a certain fixed charge amount by paid broadcasting can specify to which program it can view and listen.

(6) The invention of claim 11 can acquire the suitable collation information corresponding to a code even when two or more billing addresses of collation information exist.

---

## DESCRIPTION OF DRAWINGS

---

### [Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing the composition of the information distribution receiving system of a 1st embodiment of this invention.

[Drawing 2] It is a block diagram showing the composition of the information distribution receiving system of a 2nd embodiment of this invention.

[Drawing 3] It is a block diagram showing the composition of the information distribution receiving system of a 3rd embodiment of this invention.

[Drawing 4] It is a block diagram showing the composition of the information distribution receiving system of a 4th embodiment of this invention.

[Drawing 5] It is a block diagram showing the composition of the information distribution receiving system of a 5th embodiment of this invention.

[Drawing 6] It is a block diagram showing the composition of the information distribution receiving system of a 6th embodiment of this invention.

[Drawing 7] It is a figure showing the example of the information included in collation information in a 5th and 6th embodiment of this invention.

[Drawing 8] It is a figure showing an example of operation of the information included in collation information in a 5th and 6th embodiment of this invention and a collating part.

[Drawing 9] It is a figure showing an example of operation of the information included in collation information in a 5th and 6th embodiment of this invention and a collating part.

### [Description of Notations]

101 Code generation part

102 Broadcast transmission section

103 Center side communications department

104 Terminal side communications department

105 Broadcast receive section

106 Decoding part

201 Information server

202 Sending set

203 Modem  
204 Modem  
205 Receiving set  
206 Decoding device  
301 Code generation part  
302 Broadcast transmission section  
303 Collation information generation part  
304 Center side communications department  
305 Broadcast receive section  
306 Terminal side communications department  
307 Encryption key extraction part  
308 Decoding part  
401 Code generation part  
402 Broadcast transmission section  
403 Collation information generation part  
404 Center side communications department  
405 Broadcast receive section  
406 Terminal side communications department  
407 Collating part  
408 Encryption key extraction part  
409 Decoding part  
501 Code generation part  
502 Broadcast transmission section  
503 Collation information generation part  
504 Center side communications department  
505 Terminal side communications department  
506 Broadcast receive section  
507 Pertinent information separation part  
508 Collating part  
509 Encryption key extraction part  
510 Decoding part  
601 Timer  
602 Encryption key generation part  
603 Code generation part  
604 CS broadcasting device  
605 Collation information generation part  
606 Modem  
607 Modem  
608 CS receiving set  
609 Collating part  
610 Encryption key extraction part  
611 Pertinent information separation part  
612 Decoding part



---